

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号

特開平5-110558

(43)公開日 平成5年(1993)4月30日

(51)Int.Cl.⁵ 識別記号 庁内整理番号 FI 技術表示箇所

H 0 4 L 9/00

9/10

9/12

G 0 9 C 1/00

9194-5L

7117-5K

H 0 4 L 9/00

Z

審査請求 未請求 請求項の数1(全 9 頁)

(21)出願番号 特願平3-270982

(22)出願日 平成3年(1991)10月18日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 田代 成

神奈川県横浜市磯子区新杉田町8番地 株

式会社東芝映像メディア技術研究所内

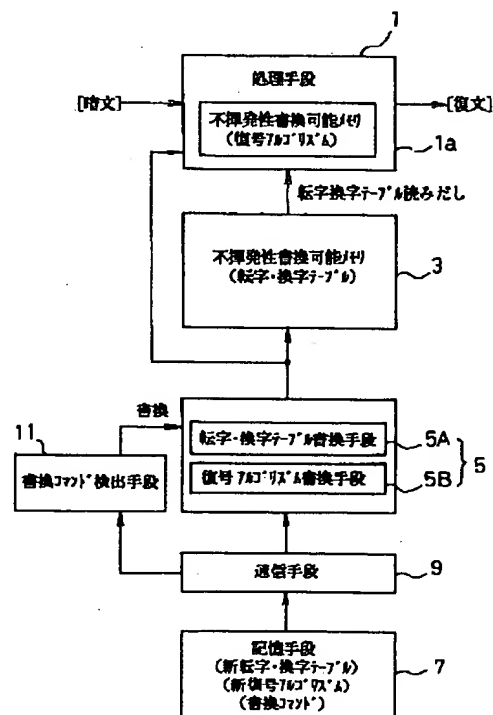
(74)代理人 弁理士 三好 秀和 (外4名)

(54)【発明の名称】 暗号処理装置

(57)【要約】

【目的】 本発明は、暗号が解読された際に暗号・復号アルゴリズム、転字・換字テーブルの一部もしくは全部を変更する手段を具備する暗号処理装置提供することを目的とする。

【構成】 本発明の暗号処理装置は、平文を暗号化して暗文とし或いは暗号化された暗文を復文化する処理手段1の一部若しくは全部を構成するプログラムの一部若しくは全部を、EEPROM3に格納するようにしている。また、暗号が解読されたような場合には、書換手段5は外部から通信手段9を介して入力される信号によってEEPROM3に格納される処理手段1の一部若しくは全部を書き換えて、当該暗号の解読に対処する。



【特許請求の範囲】

【請求項1】 平文を暗号化して暗文とし、若しくは暗号化された暗文を復文化する処理手段と、

この処理手段の一部若しくは全部を構成するプログラムの一部若しくは全部を格納する書き換え可能でかつ不揮発性の記憶手段と、

外部から入力される信号によって前記記憶手段に格納される処理手段の一部若しくは全部を書き換える書換手段とを有することを特徴とする暗号処理装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、例えば有料放送等で使用される暗号処理装置に関する。

【0002】

【従来の技術】従来、有料放送等においては平文を暗号アルゴリズムに沿って暗号化し、この暗号化によって得られる暗文が送信され、また受信の際にはこの暗文を復号アルゴリズムに沿って復号化して、各種情報を得るようにしていた。

【0003】以下、図5を参照して従来の暗号処理装置で使用される暗号・復号アルゴリズムについて説明する。この従来の暗号処理装置で、例えば暗文を復号化するには処理手段101のROM(Read Only Memory)に格納される暗号・復号アルゴリズムに沿って、ROM103に格納される転字・換字テーブルを読み出し、この転字・換字テーブルを参照して、暗号の復号化を行なうようにしていた。従って、この転字・換字テーブルを変更することが出来れば異なる暗号アルゴリズムとすることができる。

【0004】一方、この暗号化処理のほとんどが予め設定されたプログラムに従って行われることから、これら暗号・復号アルゴリズム及び転字・換字テーブルは読み出しだけで書き換えの出来ないROM上におかれるのが通常である。

【0005】

【発明が解決しようとする課題】しかしながら、これら暗号は解読される虞が多分に在り、ROM上に暗号・復号アルゴリズム及び転字・換字テーブルを設けると、暗号を解読された際に、書き換えが出来ないことから、これら暗号・復号アルゴリズム及び転字・換字テーブルの変更が不可能であり、対処することができない。

【0006】本発明は上記課題に鑑みてなされたもので、暗号が解読された場合であっても暗号・復号アルゴリズム及び転字・換字テーブルの一部もしくは全部を変更することにより対処し得る暗号処理装置を提供することを目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するため本発明は、平文を暗号化して暗文とし、若しくは暗号化された暗文を復文化する処理手段と、この処理手段の一

部若しくは全部を構成するプログラムの一部若しくは全部を格納する書き換え可能でかつ不揮発性の記憶手段と、外部から入力される信号によって前記記憶手段に格納される処理手段の一部若しくは全部を書き換える書換手段とを有することを要旨とする。

【0008】

【作用】本発明の暗号処理装置は、平文を暗号化して暗文とし或いは暗号化された暗文を復文化する処理手段の一部若しくは全部を構成するプログラムの一部若しくは全部を、書き換え可能でかつ不揮発性の記憶手段に格納するようにしている。

【0009】また、暗号が解読されたような場合には、当該記憶手段が書き換え可能であることから、書換手段は外部から入力される信号によって前記記憶手段に格納される処理手段の一部若しくは全部を書き換えて、当該暗号の解読に対処する。

【0010】

【実施例】以下、本発明の一実施例を図面に基づいて説明する。図1は本発明が適用されるデコーダの構成を説明するためのブロック図である。この図1に示す第1の実施例においては、暗号及び復号共にほぼ同様であることから、この提案が最も有効に活用される復号の場合を例に説明する。

【0011】図1において、平文が暗号アルゴリズムに沿って暗号化され、この暗号化によって得られた暗文が送信され、さらに受信された暗文が処理手段1に入力され、この処理手段1で復号アルゴリズムに沿って復号化された復文が出力される状態が示される。この処理手段1は、復号アルゴリズムを格納する不揮発性書換可能メモリ1aを有しており、この不揮発性書換可能メモリは、例えばEEPROM(Electrically Erasable Programmable ROM)が採用される。また、この処理手段1には、転字・換字テーブルを格納する不揮発性書換可能メモリ3が接続される。この不揮発性書換可能メモリ3も処理手段1と同様に、メモリに例えばEEPROM等が採用される。

【0012】この不揮発性書換可能メモリ3には、復号アルゴリズム書換手段5B及び転字・換字テーブル書換手段5Aを含む書換手段5が接続されており、この書換手段5は書換コマンド検出手段11により書換コマンドが検出されたときに処理手段1の復号アルゴリズムと不揮発性書換可能メモリ3の転字・換字テーブルの書換えをそれぞれ行うものである。

【0013】通信手段9は、デコーダとは別に設けられる、例えば放送局に設備される記憶手段7に記憶される新転字・換字テーブル、新復号アルゴリズム及び書換コマンドを前記書換手段5及び書換コマンド検出手段11に送出するものであって、通常、無線通信が用いられるが、有線放送等のように有線によるものであっても良く、さらにはデコーダに書換え用として設けられる端子

に直接接続するようなものであっても良い。

【0014】次に、本実施例における動作を暗文の復文化処理に従って説明する。常態においては、処理手段1に入力された暗文は不揮発性書換可能メモリ1aに格納される復号アルゴリズムに沿って復号化され復文化されることによって復文化処理が行われる。このとき、復号アルゴリズムは不揮発性書換可能メモリ3に格納される転字・換字テーブルを参照して実行される。

【0015】また、放送形態の変更若しくは暗号が解読される等して復号アルゴリズム或いは転字・換字テーブルを書換える必要が生じた場合には、有線若しくは無線通信による通信手段9を介して、記憶手段7に記憶される新転字・換字テーブル、新復号アルゴリズム及び書換コマンドがデコードの書換手段5及び書換コマンド検出手段11に送信される。この書換コマンドは書換コマンド検出手段11により検出され、復号アルゴリズム書換手段5B及び転字・換字テーブル書換手段5Aに復号アルゴリズム及び転字・換字テーブルの新復号アルゴリズム、新転字・換字テーブルへの書換動作を要求するものである。

【0016】従って、書換コマンドが書換コマンド検出手段11により検出されると、この検出信号が書換手段5に入力され書換え動作が要求され、書換手段5の復号アルゴリズム書換手段5B及び転字・換字テーブル書換手段5Aは処理手段1の不揮発性書換可能メモリ1aに格納される復号アルゴリズム及び不揮発性書換可能メモリ3に格納される転字・換字テーブルがそれぞれ新復号アルゴリズム及び新転字・換字テーブルに書換えられる。

【0017】上述したように、復号アルゴリズム及び転字・換字テーブルは共に不揮発性書換可能メモリ、たとえばEEPROMに格納されていることから、復号アルゴリズム書換手段5B及び転字・換字テーブル書換手段5Aを含む書換手段5によって行われる書換動作で必要に応じて適宜書き換えが可能である。また、復号アルゴリズム書換手段5B、及び転字・換字テーブル書換手段5Aには通信手段9によって記憶手段7に格納される新復号アルゴリズム及び新転字・換字テーブルが与えられることから、必要に応じた迅速な書換えが可能となる。

【0018】次に図2を参照して第2の実施例について説明する。この第2の実施例においては、暗号及び復号共にほぼ同様であることから、この提案が最も有効に活用される復号処理の場合を例に説明する。尚、図2においては理解のため復号アルゴリズムは書き換えないものとしているが、第1の実施例と同様に行うことによって復号アルゴリズムの書き換えも可能である。

【0019】この第2の実施例は第1の実施例をさらに発展させたセキュリティの高いシステムであり、暗文を復号アルゴリズムに沿って復号化して復文を出力する処理手段21と、第1の転字・換字テーブルを格納する第

1の不揮発性書換可能メモリ23Aと第2の転字・換字テーブルを格納する第2の不揮発性書換可能メモリ23Bと、転字・換字テーブル書換手段25と、新転字・換字テーブル抽出手段27と、書換コマンド検出手段31と、テーブル指定ビット抽出手段33及び切換えスイッチ35によって構成される。

【0020】この第2の実施例においては、不揮発性書換可能メモリ23A、23B内に2種類の転字・換字テーブル、すなわち第1の転字・換字テーブルと第2の転字・換字テーブルとをそれぞれ格納するようにしている。また、通常システムで使用される暗文はパケットの形で入力され、このパケットは第1の転字・換字テーブル23Aで復号できるように暗号がかけられている。また、各パケットには第1の転字・換字テーブル23Aを復号に用いるか、第2の転字・換字テーブル23Bを復号に用いるかを選択するテーブル指定ビットが設けられており、このテーブル指定ビットはテーブル指定ビット抽出手段33によって抽出され、第1の転字・換字テーブルと第2の転字・換字テーブルのどちらの転字・換字

テーブルを用いるか選択するためのスイッチ35を動作させる。その結果、当該パケットにかけられた暗号を解くための転字・換字テーブルデータが処理手段21の復号アルゴリズムに与えられる。

【0021】従って、第1の転字・換字テーブル23Aで復号できるように暗号をかけているパケットは常時送られていることから、解読される可能性が高いといえる。そこで暗号が解読された場合、暗号アルゴリズムを変更する必要があるため図3に示される転字・換字テーブルを書き換えるためのパケットが暗文として加えられている。

【0022】この暗号化入力パケットは、アルゴリズム切り替え信号41、テーブル指定ビット43、転字・変換字テーブル変更コマンド45、第1の転字・変換字テーブル変更データ47及び第2の転字・変換字テーブル変更データ49によって構成されており、この内、転字・変換字テーブル変更コマンド45、第1の転字・変換字テーブル変更データ47及び第2の転字・変換字テーブル変更データ49は転字・換字テーブルを書き換える場合のみ用いられる第2の転字・換字テーブル23Bで復号を行う暗号がかけてある。

【0023】従って、通常この第2の転字・換字テーブル23Bで復号を行う暗号を、上記第1の転字・変換字テーブル変更データ47及び第2の転字・変換字テーブル変更データ49に基づく新第1の転字・換字テーブル23Aa及び第2の転字・換字テーブル23Baに書換えられる間に解くことは不可能であることから、解読者は解読の途中で当該書換えが行われたことを知ることが出来ないまま、今回新たに送信された第1の転字・変換字テーブル変更データ47及び第2の転字・変換字テーブル変更データ49の内容を知ることがもちろん、先の

第2の転字・換字テーブル23Bで復号を行う暗号と今回の第1の転字・換字テーブル23Aで復号を行う暗号とが途中で切替わった複合的な暗号を解説しなければならなくなり、単にこの新第1の転字・換字テーブル23Aaで復号を行う暗号の解説を行うより一層の困難を伴うものとなる。

【0024】図4は、図1に示す第1の実施例若しくは図2に示す第2の実施例を並列に並べた第3の実施例を示すものである。すなわち、この第3の実施例は、図4において、平文を暗号アルゴリズムに沿って暗号化して得られる暗文をアルゴリズム切り替え検出手段61を介して、第1のアルゴリズム若しくは第2のアルゴリズムに入力し、この暗文を不揮発性書換可能メモリに格納される復号アルゴリズムに沿って復号化し、さらにこの復合化によって得られた復文を切換えスイッチ67を介して、出力するものである。

【0025】具体的には、当初は第1のアルゴリズム63によって暗号文を送っているものとするとときに、この第1のアルゴリズム63が解説されたことが判明した時点で送出される通信路上のアルゴリズム切り替え信号をアルゴリズム切り替え信号検出手段61において検出し、当該システムを第2のアルゴリズム65を使用するようにアルゴリズム切り替え信号を変更する。この間に図1に示す第1の実施例若しくは図2に示す第2の実施例のようにアルゴリズム書換コマンドを書き換えるべき暗号アルゴリズムに対して送り、このアルゴリズム（この場合は第1のアルゴリズム63）を変更する。再び第2のアルゴリズム65が解説されたことが判明した時点で、再び第2のアルゴリズム65を使用している間に書換えられた新しい第1のアルゴリズム63aを使用する

ようにアルゴリズム切り替え信号を変更すると良い。

【0026】本実施例ではこれらの操作を暗号が解説されたことが判明する毎に繰り返す事で当システムを継続的に運用しながら、暗号が解説されたことが判明した時点でハードウェアをなんら変更する事なく高いセキュリティを保った暗号システムを構築する事ができる。

【0027】

【発明の効果】以上説明したように、本発明によれば、

既存の暗号が解説された場合でも新しい暗号に変更することができるため、常にシステムのセキュリティを保持することができる。

【図面の簡単な説明】

【図1】本発明に係る第1の実施例の構成を示すブロック図である。

【図2】本発明に係る第2の実施例の構成を示すブロック図である。

【図3】図2に示す第2の実施例で使用される転字・換字テーブルの構成を示す図である。

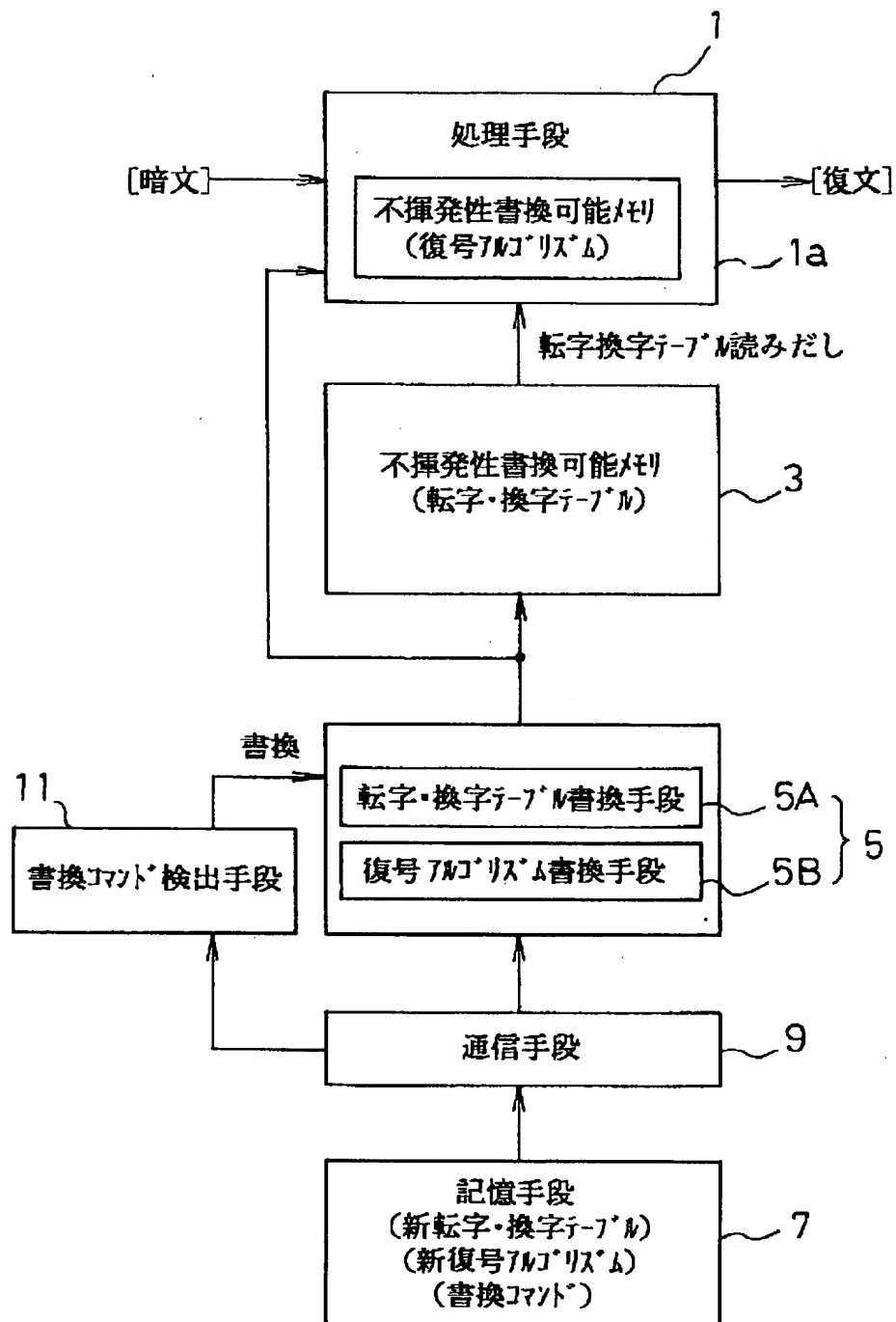
【図4】本発明に係る第3の実施例の構成を示すブロック図である。

【図5】従来の構成を示すブロック図である。

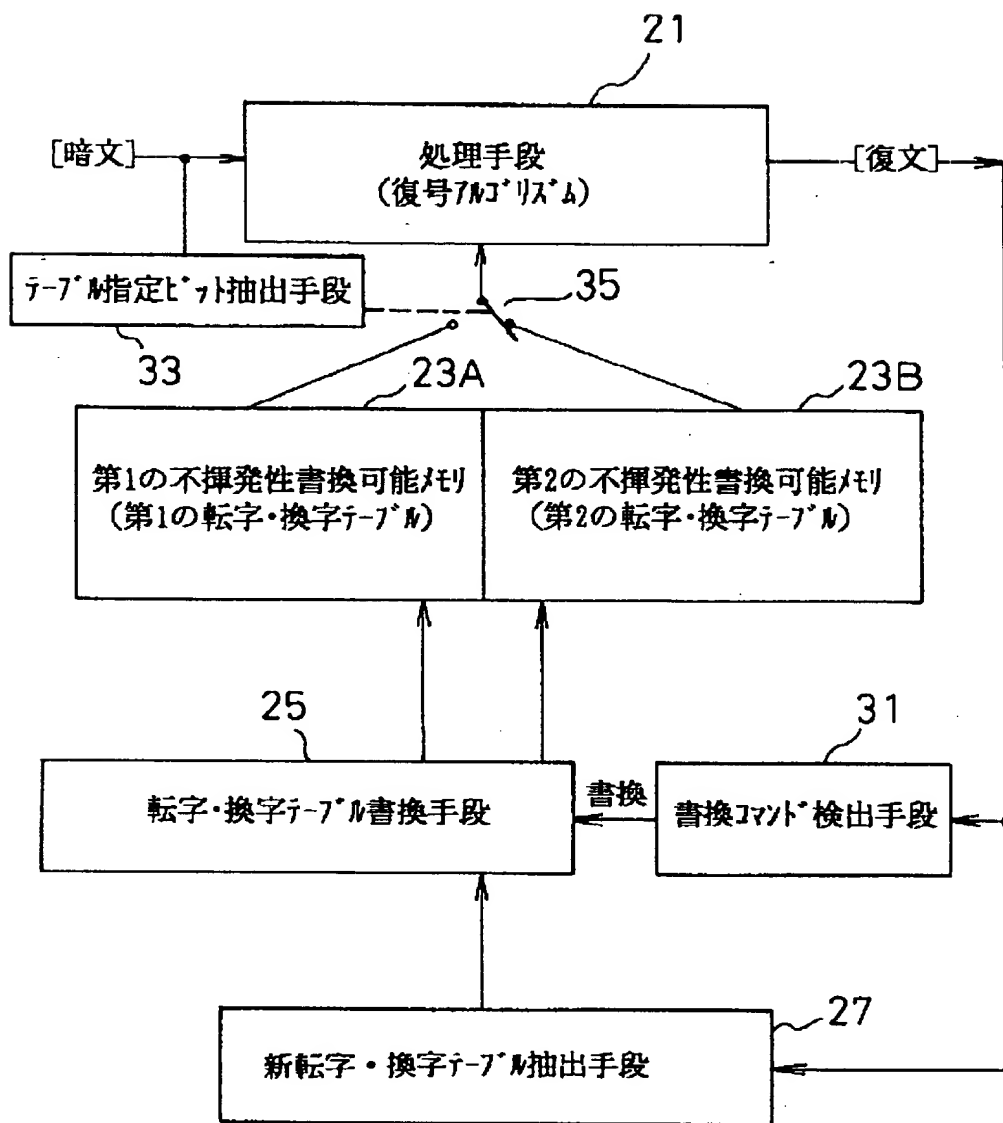
【符号の説明】

- 1 処理手段
- 3 不揮発性書換可能メモリ
- 5A 転字・換字テーブル書換手段
- 5B 復号アルゴリズム書換手段
- 7 記憶手段
- 9 通信手段
- 11 書換コマンド検出手段
- 21 処理手段
- 23A 第1の不揮発性書換可能メモリ
- 23B 第2の不揮発性書換可能メモリ
- 25 転字・換字テーブル書換手段
- 27 新転字・換字テーブル抽出手段
- 31 書換コマンド検出手段
- 33 テーブル指定ビット抽出手段
- 35 切換えスイッチ
- 41 アルゴリズム切り替え信号
- 43 テーブル指定ビット
- 45 転字・変換字テーブル変更コマンド
- 47 第1の転字・変換字テーブル変更データ
- 49 第2の転字・変換字テーブル変更データ
- 61 アルゴリズム切り替え検出手段
- 63 第1のアルゴリズム
- 65 第2のアルゴリズム
- 67 切換えスイッチ

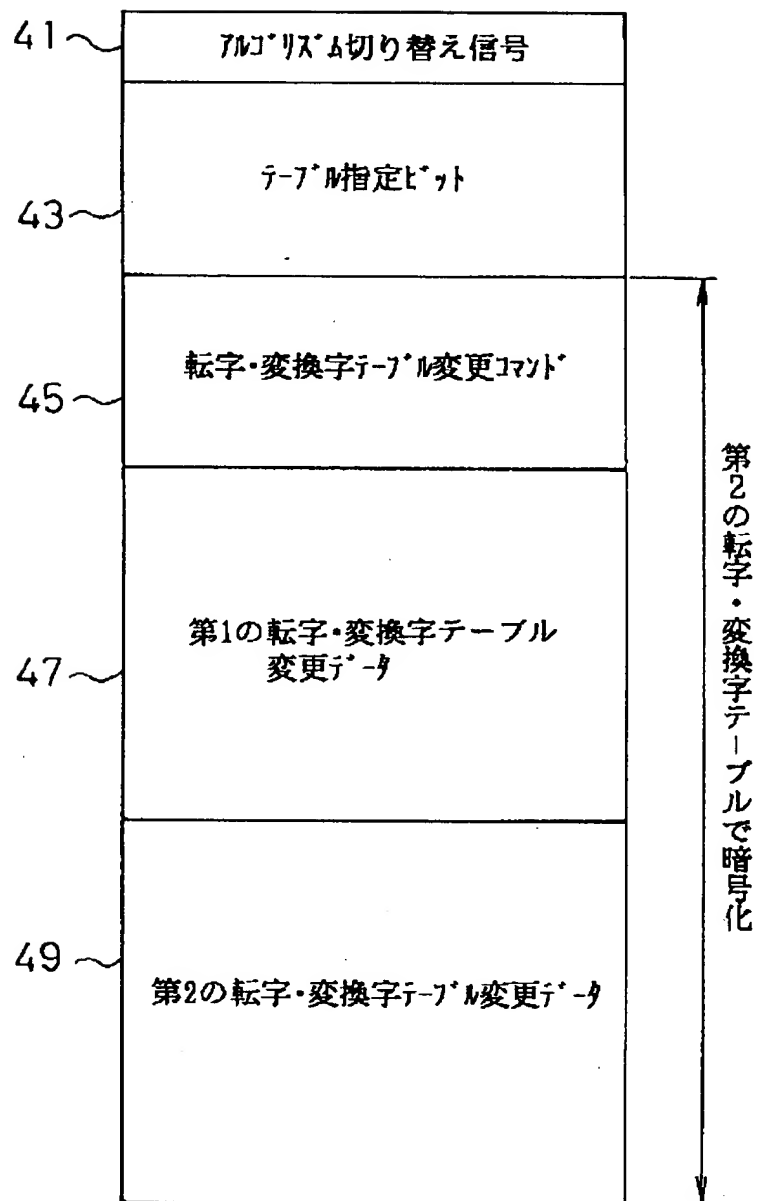
【図1】



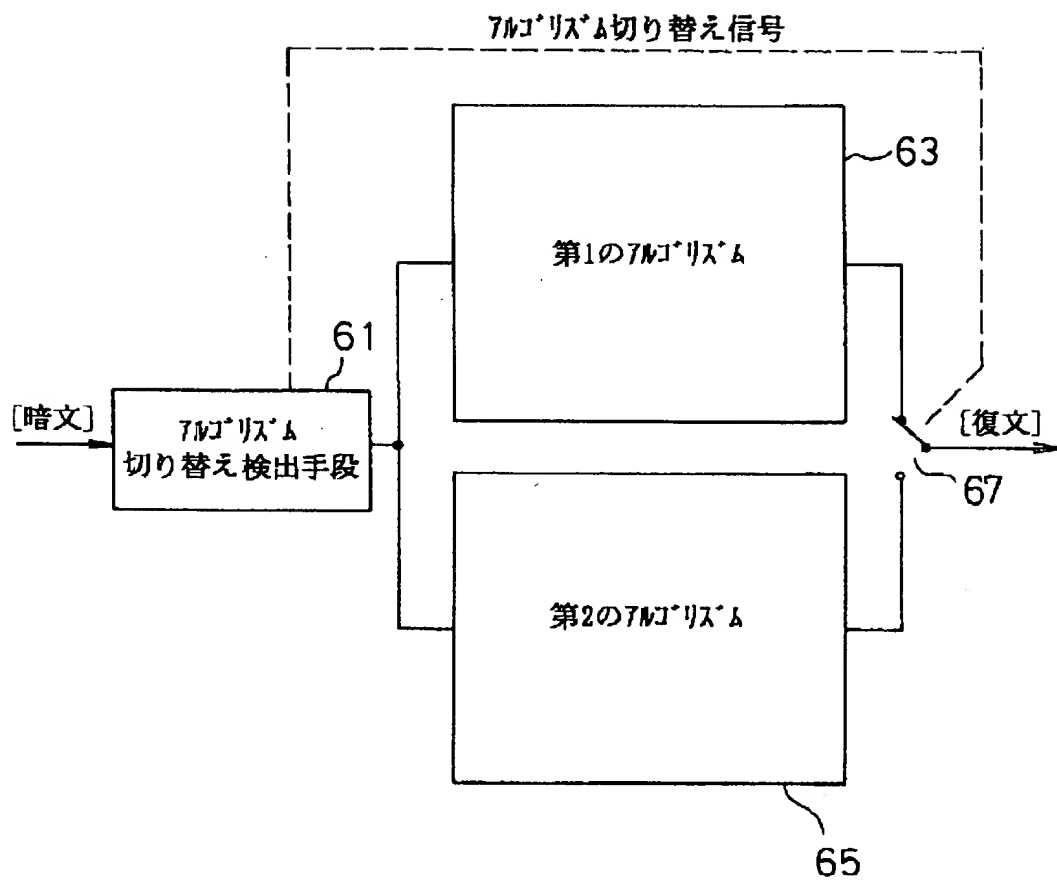
【図2】



【図3】



【図4】



【図5】

